УДК 004.056

МЕТОД ЗАХИСТУ ВІД DOS-АТАК НА ОСНОВІ ЦИФРОВОГО ВІДБИТКУ БРАУЗЕРА

М. Ю. Павлов[1], Г. О. Южакова[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В роботі запропоновано метод для протидії DoS-атакам на веб-сервер з урахуванням доцільності фільтрування та допуску окремих користувачів. Метод базується на ідентифікації «надійних» користувачів та подальшому наданні доступу таким користувачам у першу чергу. Результати роботи можуть бути використані при розробці сайтів або сервісів з високою клієнтоорієнтованістю. Розробники матимуть змогу створити інтернет-ресурс, стійкий до атак на відмову в обслуговуванні, без додаткових витрат на сторонні сервіси.

Ключові слова: HTTP-сервер, браузер, DDoS-атака, безпека, користувач

Вступ

Через постійний розвиток мережі Інтернет веб-сайти стали невід'ємною частиною будь-якої сучасної організації. Веб-сервіси забезпечують різноманітні переваги, проте їх вразливості є одним з найбільш поширених шляхів проникнення в інформаційні системи організації. Безпека сервісу не завжди є пріоритетною метою для розробника, що зумовлює появу вразливостей різного ступеня ризику. До того ж інвестиції в безпеку не забезпечують негайно видимих результатів, а покупці серверу іноді не переймаються безпекою, доки атака на нього не реалізована. Однак саме те, що робить клієнт-сервери популярними, також є тим, що робить їх найбільш вразливими до порушень безпеки. Саме розподіл послуг між клієнтом і сервером відкриває зловмисникам можливість пошкоджень, шахрайства та зловживань.

1. Безпека сучасних веб-серверів

1.1. Можливі наслідки атак на веб-сайт або сервіс

Безпека веб-застосунків є однією з найбільш серйозних проблем у контексті безпеки веб-сайтів та сервісів. Загалом, більшість веб-сайтів, доступних в Інтернеті, є вразливими до різних типів атак і постійно атакуються.

Добре виконані атаки створюють загрозу для роботи сайту, логічним наслідком цього є фінансові та репутаційні збитки.

Злочинні люди можуть використовувати цей сайт для атаки на інші ресурси як основний ресурс для надсилання спаму або DoS-атак. В результаті сайт блокується пошуковими системами та браузерами, через що користувачі програють.

Крім того напади можуть бути спрямовані на подальше «зараження» користувачів сайту, наприклад, за допомогою так званих експлойт-пакетів – використання вразливостей в браузері та його компонентів.

1.2. Вразливості сучасних веб-серверів

Найпоширенішими на сьогодні веб-серверами за обсягом використання на працюючих сайтах та сервісах є такі [1]:

1) `Apache HTTP-server` – близько 50% від загальної кількості;
2) `nginx HTTP-server` – близько 25% від загальної кількості;
3) `IIS (Microsoft)` – близько 15% від загальної кількості.

Розглядаючи вразливості цих веб-серверів можна помітити, що найбільш розповсюдженою вразливістю є так звана «`Denial of Service`», яку порівняно легко можна придбати на чорному ринку та відправити на будь-який мережевий ресурс. Тому саме для попередження цієї атаки було розроблено методику протидії.

Більшість цілей цієї атаки – це сайти, створені для заробітку. Для інтернет-магазинів простій у стані відмовлення від обслуговування в результаті приведе до зменшень замовлень і прибутку. Зазвичай такий вид нападу – атаки конкурентів. Також подібні «напади» можуть виникнути з ідейних причин. Іноді хакери потребують грошей за відновлення роботи сайту, але це рідкісні ситуації.

Саме для запобігання втрат і відтоку клієнтів запропоновано нижчеописану методику протидії DDoS-атакам на основі рейтингової системи залучення користувачів.

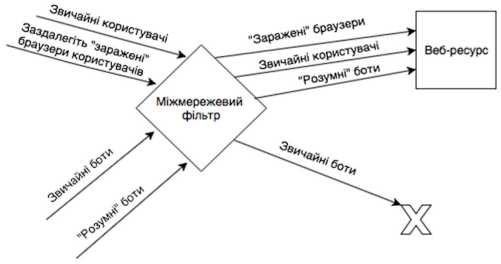

Рис. 1. Захист від DoS-атак стандартними методами

1.3. DDoS-атаки на веб-сервери

DDoS – це розподілена атака на відмову служби обслуговування. Атаки зазвичай організовуються за допомогою ботнету. Зловмисники, як правило, заражають комп'ютери звичайних користувачів з метою подальшого їх використання як ботів. Такі боти надсилають велику кількість запитів на сервер жертви.

Під час обробки мільйонів запитів сервер спочатку «уповільнює», а потім припиняє роботу. При нападі на VDS страждають фізичні сервери, що з'єднані через загальні канали трафіку VDS. В такому випадку центр обробки даних також відчуває величезне навантаження на мережевий канал, оскільки через нього проходить весь паразитний трафік.

1.4. Особливості і недоліки традиційних методів захисту

Перший недолік традиційних систем захисту від DoS-атак полягає у тому, що ця вразливість залежить не стільки від правильно налаштованих програмних засобів, скільки від потужності технічних засобів, на яких ці веб-сервери розташовані, оскільки потужність завжди є обмеженою. Тобто «розумний» фільтр може стати основним споживачем ресурсів системи, якщо він буде перевіряти всі вхідні з'єднання під час атаки, чим спровокує відмову у обслуговуванні на сервері.

Другий недолік полягає у неможливості відрізнити «розумних» ботів від справжніх користувачів без складних обчислень і витрат ресурсів серверу.

Схема захисту від DoS-атак стандартними методами наведена на рисунку 1.

Як відомо, кожна хвилина роботи комерційного сайту або сервісу коштує підприємству певних грошей, а кожна хвилина простою в стані відмови у обслуговуванні веде до значних збитків, оскільки ані нові, ані постійні користувачі цього сервісу не можуть отримати бажані послуги та, як наслідок, не генерують товарно-грошовий потік.

З цих причин в роботі пропонується метод протидії DoS-атакам з урахуванням збереження лояльності постійних користувачів. Доходи не в останню чергу залежать від кількості залучених і лояльних клієнтів. І чим більше користувачів довіряють вам, тим краще ваш бізнес буде відчувати себе в довгостроковій перспективі. Саме тому пропонований метод захисту полягає у надаванні переваги доступу до сайту або сервісу користувачам, які за певними ознаками вважаються лояльними або постійними.

У зв'язці зі стандартними методами захисту розроблений метод надасть можливість відсіювати «розумних» ботів, які нічим не відрізняються від звичайних користувачів, тим самим зменшуючи споживання ресурсів серверу.

2. Розроблений метод захисту від DoS-атак

Запропонований метод протидії атакам на відмову в обслуговуванні є простим для розуміння і складається з таких пунктів:

1) Ідентифікація користувача за допомогою цифрового відбитку браузера.
2) Запис ідентифікатора на комп'ютер користувача для полегшення роботи фільтру під час атаки.
3) Присвоєння кожному ідентифікатору певного параметру «рейтингу лояльності» (рівня довіри до цього користувача) та запис цього значення на сервер.
4) Використання параметру «рейтингу лояльності» під час перевищення ліміту запитів на сайт для аутентифікації лояльного користувача та для його відмінності від ботів.
5) Надання доступу до сайту користувачам з високим «рейтингом лояльності» і навпаки, відмова у обслуговуванні користувачів з меншим «рейтингом лояльності», за допомогою фільтру між клієнтом і сервером.

2.1. Ідентифікація за допомогою цифрового відбитку браузера

Суть техніки `Browser Fingerprinting` в тому, що код опитує браузер користувача на предмет всіх специфічних та унікальних налаштувань і даних для цього браузера і для цієї системи, для комп'ютера.

Для ідентифікації можна використати,наприклад, такі дані [2]: мова браузера; часовий пояс; розмір екрану, масив, глибина кольору екрану; системний шрифт; `SessionStorage`, `LocalStorage`, `IndexedDB`, `OpenDatabase` і інші технології стандарту `HTML5`; налаштування процесорів `doNotTrack`, `cpuClass`, тип платформи та інші дані, що стосуються користувача та платформи; інформація про плагіни.

Всі ці отримані дані об'єднуємо у рядок і передаємо на вхід хеш-функції, яка використовує їх і перетворює на 32-розрядний номер у вихідному файлі. Це і буде ідентифікатор користувача.

В цілому, можна збирати більше або менше даних для ідентифікації, тим самим збільшуючи або зменшуючи точність вгадування клієнта, але що більша точність – то більше ресурсів сервера треба виділити на цю операцію.

2.2. Формування «рейтингу лояльності» користувача

Для формування «рейтингу лояльності» кожному користувачу з ідентифікатором обчислюється значе-

ння параметру (наприклад, час, проведений на сайті або веб-сервісі), а потім цей параметр порівнюється з параметрами часу інших користувачів сайту або веб-застосунку. Також отриманий параметр можна порівнювати з середнім значенням всіх користувачів.

Отримане порівняння може мати декілька станів – наприклад: «невідомий користувач», «відомий користувач», «лояльний користувач». Його ми записуємо на сервер та асоціюємо з ідентифікатором.

В залежності від специфіки кожного окремо розглянутого сайту або сервісу параметр часу може бути замінений на будь-який інший, який відображає лояльність користувачів. Наприклад – кількість відвіданих сторінок сайту або кількість придбаного товару. Однозначно лояльними можна вважати користувачів, які пройшли процес реєстрації на сайті та навели дані про себе.

2.3. Запис ідентифікатора на бік клієнта

Для аутентифікації користувача під час перевищення ліміту запитів на сервер він повинен довести свою неналежність до ботів, які атакують сервер. Для зменшення навантаження на фільтр можна використовувати `cookie` з раніше записаним ідентифікатором (цифровим відбитком браузера).

Ефективним елементом збереження інформації в файлі `cookie` є елемент, який не можна видалити. Для цієї мети можна використати `evercookie`, що не тільки зберігає дані в сховищі, наприклад, файли `cookie`-файлів, але і використовує всі доступні репозиторії сучасних веб-браузерів. Для звичайного користувача, знання якого поверхові, видалення цих файлів `cookie` неможливе, оскільки потрібно отримати доступ до 6-8 місць на жорсткому диску для виконання ряду дій, щоб їх очистити [3].

2.4. Реалізація роботи сайту під час ймовірної DoS-атаки

Для реалізації фільтрації користувачів можна використовувати проксі-сервери, наприклад `nginx` або `lighttpd`. Режим фільтрації включається під час перевищення кількості запитів до сервера. Максимальний ліміт звернень до сервера визначається в кожному випадку окремо і залежить від технічних потужностей сервера.

У випадку, коли ліміт звернень перевищений, запускається режим роботи «ймовірність DoS-атаки». Алгоритм роботи фільтру під час цього режиму:

1) Відбувається звернення до сервера, і клієнт передає `cookie` разом з HTTP запитом; фільтр зчитує ідентифікатор, знаходить відповідний параметр «рейтингу лояльності» і, якщо параметр відповідає певним критеріям, переадресовує клієнта на сервер.
2) Якщо `cookie` відсутня, то фільтр ідентифікує браузер за допомогою цифрового відбитку і шукає збіги в базі даних відомих користувачів. Якщо збіг знайдено і параметр «рейтингу лояльності» відповідний – переадресовує клієнта на сервер.
3) В усіх інших випадках проксі-сервер відсіює запити на доступ до серверу, доки кількість звернень на сервер не повернеться до норми (нижче максимального ліміту звернень).

Рис. 2. Захист від DoS-атак з використанням запропонованого методу у поєднанні зі стандартними

Як саме буде відбуватися відхилення або пропуск користувача на сайт, залежить від окремо вибраної технології фільтру – міжмережевого екрану.

Завдяки такому алгоритму лояльні і постійні користувачі сайту або веб-застосунку можуть без перешкод користуватись веб-сервером, тоді як боти та ненадійні користувачі не матимуть доступу до сайту, тим самим знижуючи навантаження на сервер.

Це зробить DoS-атаку недоцільною у зв'язку з тим, що сайт або сервіс не втрачає своїх постійних і лояльних користувачів, а отже не втрачає свої прибутки у таких великих кількостях, як було би за умови загальної відмови у обслуговуванні для всіх користувачів.

Висновки

Результатом даної роботи є метод протидії DoS-атакам з урахуванням інтересів власника сайту та його постійних користувачів. Запропоновано простий алгоритм дій для підготовки протидії DoS-атакам, а також алгоритм дій під час ймовірної DoS-атаки.

Запропонована методологія є досить гнучкою і масштабованою, тому може бути використана для захисту сайтів та сервісів дуже широкого профілю, незалежно від їх специфіки та об'ємів відвідування.

Перелік використаних джерел

1. March 2017 Web Server Survey [Електронний ресурс]. — 2017. — Режим доступу: `http://news.netcraft.com/archives/2017/03/24/march-2017-web-server-survey.html`.
2. Browser Fingerprint – анонимная идентификация браузеров [Електронний ресурс]. — 2017. — Режим доступу: `https://habr.com/company/oleg-bunin/blog/321294/`.
3. Evercookie – самые устойчивые куки [Електронний ресурс]. — 2014. — Режим доступу: `https://habr.com/post/104725/`.